UNITED STATES PATENT APPLICATION FOR GRANT OF LETTERS PATENT

Timothy E. Dickson
Chris Whitley
INVENTORS

CARD READER MODULE WITH ACCOUNT ENCRYPTION

Withrow & Terranova, P.L.L.C.
P.O. Box 1287
Cary, NC 27512
(919) 654-4520

Docket No. 2400-369A

CARD READER MODULE WITH ACCOUNT ENCRYPTION

RELATED APPLICATIONS

[0001] The present application is a continuation-in-part of U.S. Patent Application Serial No. 09/567,689, filed May 9, 2000, entitled CARD READER MODULE WITH PIN DECRYPTION, allowed, which is herein incorporated by reference in its entirety.

FIELD OF THE INVENTION

[0002] The present invention relates to retail transaction authorization systems and, particularly, relates to card reader modules used in such systems.

BACKGROUND OF THE INVENTION

[0003] Retail transaction processing systems conventionally offer customers several different methods of payment. Payment options commonly include one or more types of payment cards. Such cards include magnetic-stripe credit and debit cards. To effect payment for a transaction, a customer causes the retail transaction processing system to read information from their payment card, such as by "swiping" the card in a magnetic card reader or placing the card in a bar-code scanner. An exemplary bar-code scanning system may be found in U.S. Patent No. 6,062,473, which is incorporated herein by reference. In turn, the retail transaction processing system contacts an outside authorization network,

submits the payment information obtained from the card, and allows or disallows the customer transaction based on return authorization information.

[0004] Frequently, a customer must enter a personal identification number referred to as a "PIN" and the retail transaction processing system transmits this PIN to the outside authorization network for verification. As the primary value of PIN use is fraud prevention, providing secure PIN handling within the retail transaction processing system is critical. U.S. Patent Nos. 5,228,084, 5,384,850, and 5,448,638, all issued to Johnson et al., and having the same Assignee as the Applicant's present invention, detail a secure PIN handling apparatus and encryption techniques in the context of a fuel dispensing system and the disclosures of these named patents are incorporated herein by reference.

[0005] In general, the aforementioned patents relate to a fuel dispensing system providing secure PIN entry at a fuel dispenser, the PIN being entered into a keypad in or proximate to the fuel dispenser. The keypad includes electronics for encrypting the PIN information using a local key. Encrypted PIN information is then passed to a site controller, which may manage the operations of one or more fuel dispensers. The site controller cooperates with a security module, with the security module providing PIN decryption capabilities to decrypt the PIN received from the fuel dispenser using a local key. After decryption, the security module re-encrypts the PIN, this time using a network key. Re-encrypted PIN information is then transferred from the site controller to an outside authorization network for PIN verification. This technique allows the network encryption key information to remain within the essentially tamper-proof secure security module

rather than it residing in the less secure electronic environment of the fuel dispenser.

[0006] Newer types of payment cards, such as electronic smart cards, have the capability to securely store verification information within the card itself. Thus, a retail transaction processing system capable of interfacing with a smart card may obtain transaction authorization based on information contained in the smart card itself. This allows so-called off-line transaction processing. In an off-line transaction, the retail transaction processing system need not communicate with an outside authorization network in real time. Rather, verification and authorization activities occur locally between the retail transaction processing system and the customer's smart card, with the retail transaction system reconciling transaction charges with the outside authorization network at a later time. Localized transaction authorization still requires positive identification of the customer and, as such, the customer is commonly required to enter a PIN in conjunction with use of their smart card. After inputting by the customer, this PIN information is transferred to the smart card, where its internal processing capabilities allow for comparison of the input PIN with stored PIN information contained in the smart card's memory.

[0007] Previous designs require transfer of input PIN information to the smart card interface in an unencrypted format—known as an "in the clear" transfer. Because of the sensitive nature of PIN information, such designs use PIN entry devices that are generally designed in a manner that prevents physical tampering with the device for the purpose of illicitly gaining access to unencrypted PIN

information input by customers. Since the input PIN information must be securely conveyed to the smart card interface so that it can be communicated to the smart card itself, past smart card interfaces integrated the PIN entry device into a common, physically secure housing. In so doing, the potential for fraud is reduced by eliminating any physically accessible wiring or communications link between the PIN entry device and the smart card interface. However, such integration is not without drawbacks.

[0008] Integrating a PIN entry device, such as a keypad, into the smart card reader complicates the overall physical design of the card reader. These design challenges are exacerbated by the fact that overall construction of the smart card reader must be substantially tamper-resistant. Tamper-resistant construction of the card reader/keypad modules significantly complicates field servicing. This is particularly unfortunate, as any system subjected to daily and sometimes careless use by consumers will fail eventually. Integrating a keypad with a smart card reader has the further drawback of limiting placement options for the keypad/card reader combination within retail transaction processing systems.

[0009] Thus, separating the card reader module from the PIN entry device offers several distinct advantages. The PIN entry device, which may be more prone to failure than the card reader module, may be made a separate, independently replaceable component in the transaction processing system. However, entering a PIN into a physically separate device introduces an opportunity for fraud because the customer PIN information must be conveyed

between different devices, which may be physically separated by several meters or more.

[0010] To eliminate this opportunity for fraud, PIN information is encrypted at its point of entry, e.g., in the input keypad. The card reader module of the present invention includes an interface adapted to receive this encrypted PIN information, along with processing capabilities necessary to decrypt such information. Thus, the present invention allows physical separation of the card reader module from the PIN entry device without compromising overall PIN handling security.

[0011] While the parent application described a secure smart card system, there has been a recent string of attacks on conventional magnetic card readers. Specifically, the magnetic card readers have been replaced in the fuel dispenser with a card reader that records account numbers. When the perpetrator collects the fraudulent card reader, the perpetrator has a ready list of credit card account numbers to use for other fraudulent activities. Thus, there is a need for a secure magnetic card reader that can communicate account information securely to the site controller.

SUMMARY OF THE INVENTION

[0012] A card reader module for inclusion within a retail transaction processing system provides off-line transaction authorization capability based on processing encrypted PIN information. The card reader module includes a communications interface for receiving encrypted PIN information from another

sub-system within the retail transaction processing system and a card interface for communicating with a customer payment card having stored PIN verification information and processing capabilities, such as an electronic smart card. A customer desiring to pay for a transaction using this type of payment card inputs their PIN into an encrypting device for secure transfer to the card reader module. In a preferred embodiment, the card reader module decrypts the received PIN information and provides the decrypted information to the customer payment card, thereby allowing it to determine the validity of the entered PIN information. Based on information returned from the customer payment card, the card reader module provides authorization information to other elements in the retail transaction processing system.

[0013] By including PIN decryption processing within the card reader module of the present invention, it may be separated from other elements in the retail transaction processing system without compromising PIN security. For example, an encrypting keypad may be used to receive customer-input PIN information. Once encrypted by the keypad, this secure PIN information may be transferred to the card reader module without requiring special security precautions regarding the communications link, e.g., wiring, between the keypad and the card reader module. Conventionally, PIN entry devices are physically integrated into card reader modules in a tamper-proof manner. This integration complicates placement of the integrated module within a customer interface included in the retail transaction processing system and increases service complexity and cost because a failure of either the PIN-entry device or card reader module requires

replacement of the entire tamper-proof assembly. Providing a separate card reader module with PIN decryption capabilities solves these aforementioned problems and preserves PIN security.

[0014] A preferred embodiment of the parent invention includes a fuel dispenser associated with a card reader module of the parent invention. An encrypting keypad, also associated with the fuel dispenser, permits customers to input PIN information that is securely transferred to the card reader module. Based on providing a customer payment card with the decrypted PIN information, the card reader module obtains authorization for a fueling transaction from the customer payment card without requiring a communications link to an outside authorization network.

[0015] As an improvement, the present invention provides a card reader with encryption capabilities, such as a magnetic card reader. When the card reader elicits an account number from a magnetic card swiped therethrough, the card reader encrypts the account number and sends the account number to a security module. The security module then decrypts the account number and allows the point of sale to use the account number as is conventional. In this manner, the account numbers are preserved in secrecy at the vulnerable point - namely, the card reader.

BRIEF DESCRIPTION OF THE DRAWINGS

[0016] Figure 1 is a simplified block diagram of a prior art fuel dispensing system.

[0017] Figure 2 is simplified block diagram of a prior art smart card reader with integrated keypad.

[0018] Figure 3 is a simplified block diagram of a fuel dispensing system in accordance with a preferred embodiment of the present invention.

[0019] Figure 4 is a simplified block diagram of a fuel dispenser in accordance with an exemplary embodiment of the present invention.

[0020] Figure 5 is a simplified block diagram of a fuel dispensing system in accordance with an exemplary embodiment of the present invention.

[0021] Figure 6 is a simplified block diagram of a preferred embodiment for the card reader module of the present invention.

[0022] Figure 7 is an isometric view for an exemplary physical embodiment of the card reader module of the present invention.

[0023] Figure 8 is a simplified logic flow diagram illustrating an exemplary logic flow of a fuel dispensing system equipped with the card reader module of the present invention.

[0024] Figure 9 is a block diagram of an exemplary embodiment of the encrypting card reader system of the present invention;

[0025] Figure 10 is a block diagram of the components of the encrypting card reader system of Figure 9; and

[0026] Figure 11 is a flow chart illustrating the function of the encrypting card reader system of the present invention.

DETAILED DESCRIPTION OF THE INVENTION

[0027] What follows is a discussion of the environment that can benefit from suitable encryption activities. The discussion of the present invention, at least as it is different than the parent application, begins with the discussion of Figure 9. However, the specification of the parent application is helpful in establishing the environment and workings that help facilitate the present invention, and is re-presented herein.

[0028] Figure 1 illustrates a prior art fuel dispensing system 100. A fuel dispenser 140 includes a PIN input device 120 and an associated magnetic card reader 104. Existing fuel dispensing systems include PIN input devices with encryption capability. Encrypted PIN information is useful in verifying credit and debit card transactions based on securely transferring the PIN between various sub-systems comprising the fuel dispensing system. However, existing systems do not incorporate smart card interfaces that are economically or conveniently integrated into such existing systems.

[0029] Customers use their magnetic-stripe payment cards 102, such as debit or credit cards, to pay for dispensed fuel. To do so, customers swipe their magnetic payment card 102 through the magnetic card reader 104 and, typically, enter their associated PIN information into the PIN input device 120 for particular types of transactions, such as debit card transactions. Because the communications link between the PIN input device 120 and the controller 110 is conventionally not protected against physical tampering or data intercept, the PIN input device 120 encrypts the customer-input PIN information using a local key before it is transmitted to the controller 110. The controller 110 receives the

encrypted PIN information and transfers it to a security module 112. The security module 112 decrypts the PIN using local key information. Then, using a different, network key, the security module 112 re-encrypts the PIN for transfer back to the controller 110 for subsequent transfer to an outside authorization network 106, as explained earlier. Authorization information returned by the authorization network 106 determines whether the controller 110 provides a fuel dispenser 140 with an authorization signal that allows the customer to conduct the fueling transaction. This system is explained in greater detail in previously incorporated U.S. Patent 5,448,638.

[0030] Intelligent payment cards, such as electronic smart cards, can eliminate the need for contacting the outside authorization network 106 for the purposes of obtaining transaction authorization. Such payment cards can provide local PIN verification and subsequent transaction authorization. The term "smart card" generally connotes an electronic payment card having internal logic processing capability and memory storage. Such capabilities allow the smart card to store and manage detailed payment account information and to perform certain transaction authorization functions. As compared to conventional magnetic-stripe cards (e.g., credit cards), smart cards support substantially more detailed interaction with a given retail transaction system adapted to interface with them. U.S. Patent No. 5,594,233 to Kenneth provides information regarding various smart card standards, smart card capabilities, and exemplary smart card interface apparatus, the disclosure of which is incorporated herein by reference. U.S. Patent No. 6,024,286 to Bradley et al. details various smart card

implementations, as well as illustrating the prior art practice of integrating PIN-entry keypads into the card reader device, the disclosure of which is incorporated herein by reference.

[0031] Thus, the inclusion of smart card interface systems within retail transaction systems provides such systems with distinct advantages. Because of the desire to minimize fraud, smart card-based transactions still typically require the card user to enter a PIN or other private identifying information in conjunction with using the smart card for transaction payment. Thus, as noted, key entry devices are commonly integrated into prior art smart card interface devices.

[0032] Figure 2 illustrates a typical prior art combination of a smart card interface device 10 that includes a keypad 12 for PIN input and a smart card unit 14 for smart card interfacing and associated processing in a typical retail transaction device. Conventionally, a physically secure module enclosure houses the smart card interface device 10. As the keypad 12 and smart card unit 14 are integrated into the same tamper-resistant housing, PIN information input into the keypad 12 is not encrypted before transferring it to the smart card unit 14. This is permissible because the communications link is itself protected from fraudulent intercept by virtue of the tamper-resistant housing. However, such integration between keypad 12 and smart card unit 14 has attendant disadvantages, particularly with regard to servicing and replacement of either the keypad 12 or smart card unit 14.

[0033] Figure 3 illustrates an exemplary fuel dispensing system 200 that incorporates the card reader module 130 (referred to in the Figures as a "smart

card reader;" the terms are used interchangeably herein) of the present invention. Fuel dispensing system 200 includes a control system (or site controller) 110, a security module 112, and a fuel dispenser 140. Fuel dispenser 140 may include the card reader module 130 in accordance with the present invention, a PIN input device 120 referred to herein by Applicant as a "SMART PAD," a magnetic card reader 104, dispensing hardware and electronics 142 (Figures 4 and 5), and an interface controller 144 (Figure 5). Note that the exemplary embodiment illustrated by Figure 3 depicts at least the SMART PAD 120 and card reader module 130 integrated within fuel dispenser 140. This configuration simply represents an exemplary option, and the card reader module 130 and/or SMART PAD 120 may be located apart from the fuel dispenser 140 while still being associated with its operation. Moreover, a single SMART PAD 120 and card reader module 130 may be associated with more than one fuel dispenser 140, with such details largely a matter of design or installation necessity.

[0034] A customer conducts fueling transactions using fuel dispenser 140. Payment for fuel may be made through magnetic card reader 104 or card reader module 130, or through alternate payment acceptors, such as wireless communication interfaces (not shown). Transactions based on a customer using a conventional credit/debit card via magnetic card reader 104 result in credit card information being passed from magnetic card reader 104 to site controller 110 via interface controller 144. Validating PIN information, input by the customer via SMART PAD 120, also passes through interface controller 144 to site controller

110. However, the PIN information is transfered to site controller 110 in an encrypted format to protect sensitive PIN data. Security module 112 decrypts the PIN information and re-encrypts it for transfer to the authorization network (along with other credit card information) via site controller 110. If the authorization network returns authorization approval to the site controller 110, it provides an authorization or dispenser enable signal to dispensing hardware and associated electronics 142 in fuel dispenser 140, thereby allowing the customer to complete their fueling transaction.

[0035] Use of the card reader module 130 in accordance with the present invention permits off-line authorization of transaction payment. When a customer uses their smart card 202 (or other type of intelligent payment card), payment authorization may be obtained locally based on information stored within the smart card 202. Smart card 202 is placed in communications with card reader 130, and SMART PAD 120 provides card reader module 130 with encrypted PIN information based on customer-input PIN data. Such information may pass to card reader module 130 via interface controller 144, but alternate embodiments provide for direct transfer of encrypted PIN information between SMART PAD 120 and card reader module 130, or indirect transfer through site controller 110 in conjunction with interface controller 144.

[0036] Enhancing the practicality of the present invention, neither SMART PAD 120 nor card reader module 130 need be initially configured with encryption keys. This minimizes security concerns associated with, for example, warehousing a supply of SMART PADS 120 and/or card reader modules 130.

Absent access control and other potentially expensive security precautions, such stored encryption keys might be compromised by determined would-be criminals. This also eliminates the need to pair specific card reader modules 130 and SMART PADs 120 based on matching encryption keys. The present invention accomplishes this by utilizing the functionality of security module 112 in determining and loading local encryption keys into SMART PAD 120 and card reader module 130, after installation into fuel dispensing system 200. Specifically, the present invention contemplates the use of a security module using an Encryption Key Exchange (EKE) algorithm to establish the encryption keying relationship between the SMART PAD 120 and card reader module 130. In this context, security module 112 is consistent with that described in the previously incorporated U.S. Patent Numbers 5,228,084, 5,384,850, and 5,448,638.

[0037] Understanding how security module 112 provides this functionality requires some understanding of cryptography, and a more detailed understanding of the EKE and its variants. Bruce Schneier provides a comprehensive introduction to cryptography in his book, "*Applied Cryptograpy*", Second Edition, published in 1996 by John Wiley & Sons, Inc., the entirety of which is incorporated herein by reference. In particular, see pages 518-522 of this book for a specific presentation of the EKE and its uses. EKE provides secure authentication in a computer network environment. Using EKE, two computer systems use a shared secret key to encrypt a randomly generated public key. EKE provides a method for securely establishing a keying

relationship between two devices or entities that do not share any secret data. Both the SMART PAD 120 and card reader module 130 may be thought of as "networked entities," albeit indirectly, with security module 112. Through communication of non-secret data between the two networked entities, a shared key may be established. This shared key may then be used to generate a common (and private) session key that is used by both systems to encrypt information exchanged during the session. In an exemplary embodiment, encryption key distribution between security module 112, SMART PAD 120, and card reader module 130 is based on the well known Diffie-Hellman protocol, which offers, among other advantages, a simplification of the EKE algorithm.

[0038] Thus, in the context of the present invention, the use of EKE allows the security module 112 to determine, in cooperation with SMART PAD 120 and card reader module 130, encryption key information used to encrypt and decrypt customer-input PIN information. Because this is done after a particular SMART PAD 120 and card reader module 130 are placed in communication with a particular security module 112, the need to inject secret encryption keys into either the SMART PAD 120 or card reader module 130 is eliminated.

[0039] SMART PAD 120 is preferably housed in a tamper-resistant enclosure suitable for mounting within the fuel dispenser 140, or other retail transaction system. By design, the SMART PAD 120 prevents access to internal keypad wiring that carries input unencrypted PIN information. As explained above, SMART PAD 120 encrypts the input PIN information using a local encryption key.

Once encrypted, the SMART PAD 120 transfers the PIN information to various other sub-systems within the fuel dispensing system 200.

[0040] The card reader module 130 of the present invention reads intelligent payment cards, such as electronic smart cards 202. With the card reader module 130 providing an interface to the customer's smart card 202, the site controller 110 can conveniently enable the fuel dispenser 140 based on authorization information determined locally in cooperation with the smart card 202. In this scenario, the site controller 110 need not contact an outside authorization network 106 for PIN verification purposes. The customer physically interfaces their smart card 202 with the card reader module 130 and then enters their PIN or other identity verification data into the SMART PAD 120. Once encrypted within the SMART PAD 120, this PIN information is transferred to the site controller 110, which relays it to the card reader module 130. The card reader module 130 decrypts the encrypted PIN information, with the decrypted PIN information processed in cooperation with the customer smart card 202 to determine whether the transaction is authorized. Transaction authorization is based, in part, on verifying the customer-input PIN information against information stored on the customer smart card 202. Depending upon the smart card 202 implementation, this verification consists of the card reader module 130 decrypting the customer-input PIN information encrypted by the SMART PAD 120 and transferring this decrypted PIN information to the smart card 202 for on-card verification, or consists of the card reader module 130 receiving stored

verification information from the smart card 202 in response to a request for such data and performing the customer-input PIN verification itself.

[0041] As noted, before the customer-input PIN can be verified, card reader module 130 must decrypt the PIN information it receives directly or indirectly from SMART PAD 120. If the customer has entered valid PIN information and if the smart card 202 contains available payment credit, the site controller 110 provides the fuel dispenser 140 with an authorization signal, thereby allowing the customer to proceed with the fueling transaction.

[0042] Preferably, the SMART PAD 120 and card reader module 130 are each contained in a tamper-resistant module housing. All, or at least a critical portion of the electronics comprising the functional portions of the card reader module 130 (and SMART PAD 120) are preferably disabled in response to any attempted tampering. Such disabling may be mechanical, such as bonding critical circuit traces to interior elements of the housing in a manner that breaks them upon opening the enclosure. As an alternative, or in combination with this, certain data codes that must be present for operation may be stored in a memory that is erased or corrupted upon opening the housing. Of course, many other suitable methods exist for preventing access to the interior of the card reader module 130 and SMART PAD 120.

[0043] Figure 3 additionally illustrates an economic advantage of the card reader module 130 of the present invention. Particularly, Figure 3 illustrates the use of a magnetic card reader 104 for use with a conventional credit/debit card 102 in combination with the card reader module 130 of the present invention. As

earlier detailed, the SMART PAD 120 provides encrypted verification indicia to the site controller 110 (or other sub-systems within the fuel dispensing system 200) in conjunction with credit/debit card transactions conducted using the magnetic card reader 104. Encrypted information from SMART PAD 120 is also used for transactions conducted using card reader module 130. Thus, an exemplary embodiment of the present invention uses a single keypad (SMART PAD 120) for transactions involving either the magnetic card reader 104 or the card reader module 130 of the present invention.

[0044] Figure 4 illustrates another exemplary embodiment of the present invention. In Figure 4, the fuel dispenser 140 integrates the site controller 110, the SMART PAD 120, the card reader module 130, and the dispensing hardware and associated electronics 142. In this embodiment, the fuel dispenser 140 is capable of stand-alone, off-line transaction authorization based on interfacing with a customer smart card 202 via card reader module 130. Note that the configuration of Figure 4 may use the security module 112 illustrated in Figure 3 in a similar manner. In this case, encryption key information is handled between SMART PAD 120 and card reader module 130 in cooperation with security module 112 as previously explained.

[0045] Figure 5 illustrates another exemplary embodiment of the present invention. In Figure 5, the fuel dispenser 140 again integrates the SMART PAD 120, the card reader module 130, the dispensing hardware and associated electronics 142, along with an interface controller 144. Note that the fuel dispenser controller 144 may be associated with other payment interfaces (not

shown), such as a magnetic card reader or wireless payment interface, and may also be associated with the fuel dispenser 140's customer interface (not shown). In this embodiment, the SMART PAD 120 directly transfers encrypted PIN information to the card reader module 130 for verification processing. The fuel dispenser controller 144 receives information from the card reader module 130 indicating whether the given transaction is authorized. This information is transferred to the site controller 110, which, if the transaction is authorized, provides an authorization signal used by fuel dispenser controller 144 to enable the dispensing hardware and associated electronics 142. As with Figures 3 and 4, the exemplary configuration of Figure 5 may use a security module 112 in association with encryption/decryption key operations.

[0046] The above illustrations depict various physical configurations of fuel dispensing systems including the card reader module 130 of the present invention. The location of the card reader module 130, whether in the fuel dispenser 140, or remotely located, is not critical to practicing the present invention. Nor is it critical as to whether the card reader module 130 receives encrypted PIN information directly from the SMART PAD 120, or indirectly from another electronics subsystem, such as the site controller 110. Further, the specific architecture of the fuel dispenser 140, including its interconnection with site controller 110, is not critical to practicing the present invention. The card reader module 130 of the present invention includes the ability to decrypt encrypted PIN information received from an external system. This allows the communications link or wiring between the external system and the card reader

module 130 to be unprotected, thereby significantly reducing the expense associated with installing, maintaining, or modifying the communications link.

[0047] Figure 6 provides more detail regarding the card reader module 130 in a preferred embodiment of the present invention. A communications interface 132 provides a connection between the card reader module 130 and the device from which it receives the encrypted PIN information. As noted, the card reader module 130 preferably receives this information directly from SMART PAD 120, or from an associated site controller 110. The card reader module 130 also provides an authorization information output via communications interface 132, for providing authorization information to an associated system, such as the site controller 110 or the fuel dispenser controller 144. Although Figure 6 depicts different signal lines for the incoming encrypted PIN information and outgoing authorization information, the card reader module 130 may actually have a single interface for both incoming and outgoing information.

[0048] Internally, a decryption processor 136 receives the encrypted PIN information through the communications interface 132. The decryption processor 136 decrypts this information and provides the decrypted PIN and associated data to the authorization processor 134. The authorization processor 134 communicates with the customer smart card 202 through the card interface 138.

[0049] In a preferred embodiment, the authorization processor 134 provides the smart card 202 with the decrypted PIN information and relies on the smart card 202 to determine transaction authorization based on the decrypted PIN information. Thus, the smart card's processing capability is advantageously used

for the purpose of determining off-line transaction authorization. Based on comparing the decrypted PIN information it receives from the authorization processor 134 with its own internally stored PIN data, the smart card 202 determines whether to authorize or not authorize the fueling transaction. The smart card 202 provides authorization processor 134 with this authorization information and, in turn, authorization processor 134 outputs the authorization information via communications interface 132. In other exemplary embodiments, the smart card 202 provides the authorization processor 134 with its stored PIN information and the authorization processor 134 compares the stored PIN information received from the smart card 202 with the decrypted PIN information received from the decryption processor 136. Based on this comparison, the authorization processor 134 provides output authorization information via communications interface 132.

[0050] Figure 7 depicts an exemplary physical embodiment of the card reader module 130 of the present invention. The card reader module 130 electronics and wiring terminations are physically secured within a tamper-resistant housing 710. Interface wires 720 (referred to in the Figures as physically unsecured wiring 720) exit the tamper-resistant housing 710 and connect with associated subsystems, such as the SMART PAD 120 or the site controller 110. Because these interface wires 720 do not carry any sensitive customer identification information in an unencrypted format, they are not protected between the card reader module 130 and any associated, external devices.

[0051] Figure 8 illustrates simplified flow logic outlining operation of the fuel dispensing system 200 in accordance with a preferred embodiment of the present invention. Operation begins (block 810) with the fuel dispensing system 200 in a state associated with the start of a fueling transaction. In this state, the customer has indicated to the fuel dispensing system 200 their desire to conduct a smart card-based fueling transaction. As such, the customer inputs their PIN into SMART PAD 120 (block 820). Subsequent to completion of PIN input operations, SMART PAD 120 encrypts the input PIN (block 830). SMART PAD 120 then transfers the encrypted PIN information (block 840) either directly or indirectly to the card reader module 130.

[0052] The card reader module 130 decrypts the encrypted PIN information (block 850) for comparison with PIN information stored in the smart card 202 (block 860). Based on this comparison, the card reader module 130 determines authorization information (block 870), and transfers the authorization information to the site controller 110 (block 880). The site controller 110 processes the authorization information to determine whether the transaction is authorized (block 890). If the transaction is not authorized (block 890), the fuel dispensing system 200 displays a message (block 940) via a customer interface display included in the fuel dispenser 140 indicating that the transaction is disallowed and transaction processing ends (block 950). (Note that the fuel dispensing system 200 may provide the customer with other payment options if the smart card transaction is disallowed, but this processing is not illustrated.)

[0053] If the authorization information indicates that the transaction is authorized (block 890), processing continues with the site controller 110 enabling the fuel dispenser 140, thereby allowing the customer to dispense fuel (block 900). Subsequent to completion of the fuel dispensing operations, the site controller 110, in cooperation with the fuel dispenser 140, totals the charges associated with the transaction (block 910). Charges are presented to the smart card 202 for debiting from the customer's electronic account (block 920) and the site controller 110 records payment information and associated charges (block 930). Once payment is secured, the transaction processing ends (block 950).

[0054] The present invention may, of course, be carried out in other specific ways than those herein set forth without departing from the spirit and essential characteristics of the invention. For example, the card reader module 130 of the present invention may be associated with one or with multiple fuel dispensers 140. Further, the card reader module 130 may receive encrypted information from a variety of sources, such as directly from the SMART PAD 120 or another encryption device, or from the site controller 110. Indeed, the card reader module 130 of the present invention may be advantageously included in retail transaction systems apart from the fuel dispensing environments illustrated herein. Thus, the card reader module 130 of the present invention can impart flexibility to these general retail transaction-processing systems by allowing separation between the keypad (or other pin entry device) and the smart card interface.

[0055] Turning now to the focus of the present invention, Figure 9 shows a fuel dispenser 140 which includes a card reader 104A according to the present invention along with the SMART PAD 120. The card reader 104A is preferably a magnetic card reader, although it could be a smart card reader analogous to card reader module 130. The card reader 104A receives the account information from the magnetic card 102. The account information may include sensitive account information such as a credit card number or a debit card account number. The card reader 104A encrypts the account information and sends it to the site controller 110. Optionally, the encrypted account information may pass through the interface controller 144, although it may be passed directly to the site controller 110. Interception of the sensitive information is unlikely at the interface controller 144 because the information is already encrypted by the card reader 104A.

[0056] Once at the site controller 110, the site controller 110 may decrypt the information with the security module 112. The account information may then be re-encrypted with a network encryption key and sent to the authorization network 106 as is conventional.

[0057] It should be appreciated that during the re-encryption the account information may be coupled to PIN information from the SMART PAD 120 if needed, such as, for example, during an authorization sequence for a debit card. It should also be appreciated that the card reader 104A may have the encryption key injected during manufacturing, or, more preferably, through the EKE scheme described above with respect to the SMART PAD 120.

[0058] While the present invention is well suited for magnetic card readers, it is also possible that a smart card reader such as card reader module 130 could also benefit from the present invention. For example, if the smart card 202 did not have sufficient funds stored thereon to authorize a transaction, the smart card 202 could alternatively provide account information so that authorization using the authorization network 106 could be secured. In this manner, the card reader module 130 would be in possession of sensitive account information in the same manner that the card reader 104A had sensitive account information. Thus, the card reader module 130 could similarly encrypt the account information and send it to the site controller 110 for use as needed. Again, the card reader module 130 could be equipped with the encryption key through the EKE scheme described above.

[0059] It should be appreciated that the card reader 104A is self-contained and preferably tamper proof. The tamper proofing mechanisms described above are suitable for tamper proofing the card reader 104A. In this manner, the account information is not vulnerable either in the card reader 104A or on the transmission lines to the site controller 110. In the first place, the structure of the card reader 104A protects the account information and in the second place, the encryption protects the account information.

[0060] A more detailed block diagram of the card reader 104A is presented in Figure 10. Specifically, the card reader 104A may include a card interface 50 that is adapted to read account information from the card. The account information is passed to an encryption module 52 that encrypts the account

information. The encrypted account information is passed to a processor 54 that controls the card reader 104A, which in turn passes the encrypted account information to a communications module 56. The communications module 56 passes the encrypted account information to the site controller 110.

[0061] In the event that the card reader 104A is a smart card reader, an optional decryption module 58 may be present to decrypt encrypted PIN information as explained above. The processor 54 would then act as the authorization processor 134 as needed.

[0062] A flow chart illustrating the functionality of the present invention is presented in Figure 11. The process starts when the customer inserts the card into the card reader 104A (block 1000). The card may be a magnetic card 102 or a smart card 202. The card reader 104A receives account information from the card (block 1002). The card reader 104A then encrypts the account information (block 1004) and sends the encrypted account information to the site controller 110 (block 1006). Since the account information is encrypted, the information may be sent over insecure lines without worry about interception. The security module 112 then decrypts the encrypted account information and re-encrypts the account information for transfer to the authorization network 106 (block 1008). The account information may be coupled with PIN information or other information as needed or desired by the authorization network 106.

[0063] The authorization network 106 replies with an authorization signal (block 1010) and the transaction is authorized at the dispenser (block 1012).

[0064] The present embodiments are, therefore, to be considered in all respects as illustrative and not restrictive, and all changes coming within the meaning and equivalency range of the appended claims are intended to be embraced therein.